Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

An Investigation of Risk Management Issues in the Context of Emergency Response Systems

Jin Ki Kim
University at Buffalo, The State University of New York, jkkim3@buffalo.edu

Raj Sharman
SUNY Buffalo, rsharman@buffalo.edu

H. Raghav Rao
SUNY Buffalo, mgmtrao@buffalo.edu

Shambhu Upadhyaya
SUNY Buffalo, shambhu@cse.Buffalo.EDU

An investigation of risk management issues in the context of emergency response systems

Jin Ki Kim
State University of New York at Buffalo,
Management Science and Systems
jkkim3@buffalo.edu

Raj Sharman
State University of New York at Buffalo,
Management Science and Systems
rsharman@buffalo.edu

H. Raghav Rao
State University of New York at Buffalo,
Management Science and Systems
& Computer Science and Engineering
mgmtrao@buffalo.edu

Shambhu Upadhyaya
State University of New York at Buffalo,
Computer Science and Engineering
shambhu@cse.buffalo.edu

ABSTRACT

Since the September 11, 2001 terrorist attacks, efforts to enhance risk management have taken on increased importance both at the national and state levels. Most current incident response systems do not consider risk as part of the decision making scenario. To effectively mitigate multi-incident coordinated terrorist threats, it is important to consider risk in incident management systems. Based on the review of previous literature, this study proposes a theory-based risk framework for an emergency response system. Proof of concept is provided by applying the framework to two separate existing incident management systems - the urban search-and-rescue system and the biological detection systems.

Keywords

Risk management; emergency response system; risk assessment; theory of shortage; theory of allocation; cyber terrorism

INTRODUCTION

Since the September 11, 2001 terrorist attacks, efforts to enhance risk management have taken on increased importance both at the national and state levels. Most current incident response systems do not consider risk as part of the decision making scenario.

This study aims at investigating risk management issues in the context of emergency response systems. We review various existing emergency or incident management systems, analyze risk management tools, and articulate the risks of emergency response systems.

INCUMBENT INCIDENT MANAGEMENT SYSTEMS

Various incident management systems have been developed over the past several years and are available for use today. Each of these systems has its own differing objectives, features, characteristics, and structures respectively. In this section we describe some of the most prominent one.

In the late 1960s, the Office of Emergency Preparedness (OEP)[1] was given the responsibility to build an Emergency Management Information System for the Wage Price Freeze (EMISARI). EMISARI was used for transportation strikes, coal strikes, petroleum, chlorine, and natural gas shortages, and more severe natural disasters. EMISARI allowed 200 to 300 users scattered throughout the country to exercise a coordinated response to crisis situations (Turoff, 2002). The system design focused on group communication process and how humans gather, contribute, and utilize data in a time-urgent manner. The objective of the system was to allow distributed and probably dispersed groups of people to track and coordinate their

[1] The OEP was the civilian agency that could exert command and control over all federal resources upon the declaration of a federal emergency. In emergency situations the OEP could take over direct command and control of any federal resources (Turoff, 2002).

activities as needed. A key to the performance of the system was its ability to keep track of what people are actually searching for and provide a list of what is being searched for and not found (Turoff, 2002).

Another example of incident management is the Center for Research on Unexpected Events (CRUE), whose mission is to help transform the United States government's ability to respond to unexpected events by building on revolutionary IT development systems. CRUE's major research groups cover agents, sensor networks and fusion, situation awareness, geographic information systems, and information integration. The new research, technology, and infrastructure might initially be aimed at improving the ability to respond to unexpected disasters (Arens and Rosenbloom, 2003).

On February 28, 2003, the President issued the Homeland Security Presidential Directive (HSPD)-5, Management of Domestic Incidents, which allows the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). NIMS integrates best practices that have proven effective over the years into a comprehensive framework for use by incident management organizations in an all hazards context nationwide (U.S. Department of Homeland Security, 2004).

Among the different kinds of possible attacks, potential for biological attacks and chemical warfare are perceived as more likely. Biological agents can be manufactured in facilities that are inexpensive to construct, that resemble pharmaceutical, food, or medical production sites, and that provide no detectable sign that such agents are being produced. The biological agents are likely to be used in a terrorist attack (Fatah, Barrett, Arcilesi, Ewing, Lattin, and Moshier, 2001).[2]

Incident systems	Objectives	Features or Characteristics	Citations
EMISARI	Designed to deal with severe disasters such as transportation (coal) strikes, petroleum (chlorine, natural gas) shortages	Search experts Group communications (200-300 users) Collaborative Delphi process	Turoff (2002)
CRUE	Response to unexpected events	IT development Geographic information systems Information integration	Arens and Rosenbloom (2003)
COPLINK	Sharing law enforcement-related information	Multiple data sources Different user interfaces Concept space	Atabakhsh, Schroeder, Chen, Chau, Xu, Zhang, and Bi (2001); Chen, Zeng, Atabakhsh, Wyzga, and Schroeder (2003); Wang, Chen, and Atabakhsh (2004)
NIMS	Integration existing best practices into a consistent, nationwide approach to domestic incident management	Integration existing practices of incident system Consistent nationwide to enable Federal, State, and local governments and private-sector and nongovernmental organizations	U.S. Department of Homeland Security (2004)

Table 1. Incumbent Incident Management Systems

*: EMISARI: Emergency Management Information System for the Wage Price Freeze

CRUE: Center for Research on Unexpected Events

CRASAR: Center for Robot-Assisted Search and Rescue

NIMS: National Incident Management System

[2] For detail, refer to Fatah, et al. (2001).

Components of Incident Management System

Typically the core activities for incident management system consist of rapid detection, precise diagnostics, and right response. First of all, detecting early is the most important thing in overcoming the emergent situation. A good monitoring system is required for better incident management systems. The second aspect is precise diagnosis. It is a basis for accurate response, as shown in the following step.

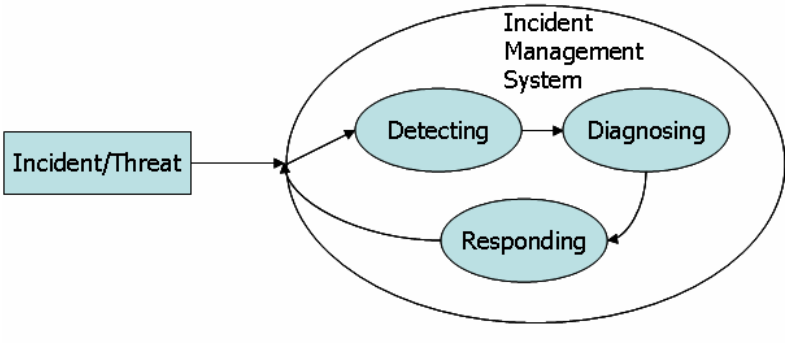

Figure 1. Components of Incident Management Systems

For instance, biological agent detection systems generally consist of four components: the trigger/cue, the collector, the detector, and the identifier. Figure 1 shows a flow diagram for a typical point detection automated architecture system.

Trigger technology is the first level of detection that determines any change in the particulate background at the sensor indicating a possible introduction of biological agents. Detection of an increase in the particulate concentration by the trigger causes the remaining components of the detection system to begin operation. Sampling of the biological agent is a crucial part of the identification system. Once a sample has been collected/concentrated, it must be determined if the particulates are biological or inorganic in origin. To accomplish this, the sample is passed to a generic detection component that analyzes the aerosol particles to determine if they are biological in origin. This component may also classify the suspect aerosol with broad categories. If the sample exhibits characteristics of biological particles, it is passed through to the next level of analysis. If the sample does not exhibit such characteristics, it is not passed to the next level of analysis, thereby conserving analytical consumables. An identifier is a device that specifically identifies the type of biological agent collected by the system. Identifiers are generally limited to a pre-selected set of agents and cannot identify agents outside of this set without the addition of new identifier chemistry/equipment or preprogramming (Fatah et al., 2001).

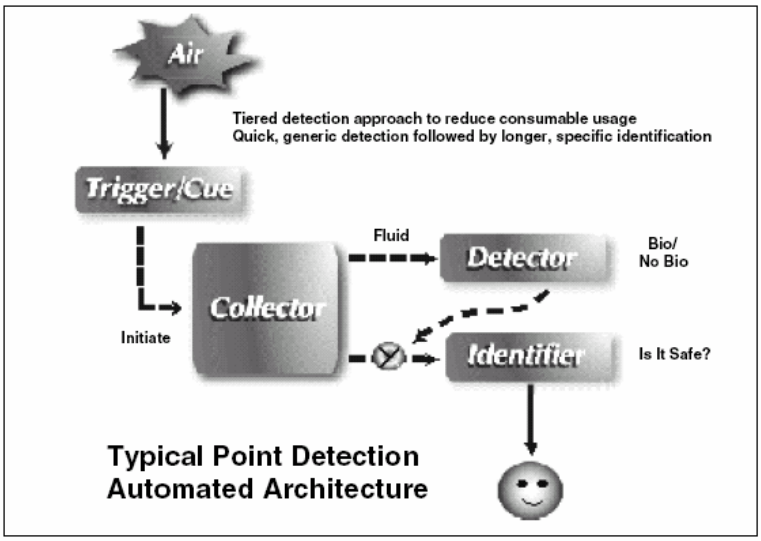

Figure 2. Typical point detection automated architecture (with a combined trigger/cue)

Source: Fatah et al. (2001).

Arens and Rosenbloom (2003) propose six future research agendas for incident management systems: encyclopedic digital collections, a grid of unlimited computation, rapidly deployable sensors and effectors, a pervasive, secure communications infrastructure, integrated analysis, fusion, and learning, virtual organizations, legal framework.

PRIOR LITERATURE

Existing literature reveals that there are a plethora of tools for risk assessment. Further the literature also shows that quantitative risk assessment (QRA) was first applied to applied to large technological systems nearly thirty years ago. Since then, we have seen many methodological advances and applications to nuclear power reactors: probabilistic risk assessment (PRA), space systems, performance assessment, and incinerators of chemical munitions (Apostolakis, 2004). Apostolakis (2004) discusses the use of quantitative risk assessment (QRA) in decision-making regarding the safety of complex technological systems. The insights gained by QRA are compared with those from traditional safety methods and it is argued that the two approaches complement each other. The importance of risk-informed rather than risk-based decision-making is emphasized (Farrow, 2004).

To capture the multiple dimensions and perspectives of a system, Haimes (1981, 2004) introduces hierarchical holographic modeling (HHM). Haimes (2002) also offers a holistic risk assessment and management framework for modeling the risks of terrorism to the homeland. Two major interconnected systems are addressed: the homeland system and the terrorist networks system. In modeling the two systems, the centrality of state variables is highlighted. Paté-Cornell (2002) presents a classic probabilistic Bayesian model used in engineering risk analysis, which can be helpful in the fusion of information because it allows computation of the posterior probability of an event given its prior probability and the quality of the signal characterized by the probabilities of false positive and false negative. However, some critical issues remain such as (a) the choice of the signals that are carefully monitored, (b) quick access to information when a source has been located and, (c) the constitution of an extensive database or system that link existing databases allowing for storing and updating the information in a useful way.

Wulf, Haimes, and Longstaff (2003) develop a roadmap toward modeling the complex structure, which consists of the following four systems: Homeland, Terrorist networks, Socioeconomic and cultural environment, and geopolitical environment that sustain terrorism. Risk analysis has already played some role informally, but a much larger and formal one is needed since it has a centrally important role for protecting the world against the terrorism (Deisler, 2002). How one can link the tools of risk assessment and knowledge of risk perception to develop risk management options for dealing with extreme events is also a critical issue (Kunreuther, 2002).

Generally, risk analysis is derived from risk assessment and risk management. Risk assessment is an established methodology for environment and public health issues (Farrow, 2004). It is still not easy to assess the amount of risk. The Risk Assessment Cube is a simple and useful example to estimate the amount of risk. There are three components in the risk assessment cube: probability of an incident, outcome severity, and duration of impact (Volonino and Robinson, 2004).

However the above approaches are limited in that they does not account for several parameters. In this paper we anchor our proposed framework on the economic theory of shortages. The next subsection provides a brief elaboration of the related concepts.

Traditional theory of allocation deals with the fundamental question of how available productive resources can be used to the greatest advantage in the production of goods and services. However, the situation that the emergency response systems are facing does not directly fit the situation that the traditional economists have taken. When strong emotions are involved, people tend to focus on the "badness" of the outcome, rather than on the probability that the outcome will occur. The resulting probability neglect helps to explain excessive reactions to low-probability risks of catastrophe (Sunstein, 2003). Emergency situations have considerable ambiguity and uncertainty about the likelihood of their occurrence and their potential consequences (Kunreuther, 2002). This situation is similar to that of economics of shortage. Shortage is a persistent feature of all economies. Consequences of shortage, such as misallocation of resources, delaying of completions of projects, queuing, hoarding, rent-seeking, are widely observed and extensively analyzed (Kornai, 1980; Qian, 1994). This area deals with a question of why there is shortage under governments which have immense power to allocate goods and services (Qian, 1994). Haskel and Martin (1993) show that the increase in skill shortages over the mid-1980s reduced productivity growth.

The theory of shortage deals with the several sub issues.

- Imperfect Information and lack of Information: The more imperfectly informed a consumer, the greater the friction in adjustment and the more intensive will be the shortage or the greater the slack. Imperfect or partial information does not lead to optimized solution for emergency response system. Often imperfect information leads to wrong

decisions. Information sharing in the emergency response system can lead to creation of more correct information with cross-checking (Kornai, 1980; Qian, 1994).

- Resource constraints – Inputs: Shortage means that inputs required for the fulfillment of some serious intention are not available resulting in suboptimal decisions. Resources that are needed in an emergency situation are usually short. Therefore, under the environment of resource shortage, efficient resource allocation is a crucial factor for emergency response systems (Haskel and Martin, 1993; Kornai, 1980; Qian, 1994).
- Resource constraints – Local infrastructure: With limited infrastructure as is the case in many emergency situations deciphering how to optimize the infrastructure is important in the use of existing emergency response systems. Organization and coordination of scattered resources in the system impacts the efficiency. Infrastructure that is a basis for various social systems is also vulnerable to several threats or risks. The infrastructure can be often a target for offenders because the paralyzing of infrastructure strikes the whole social system a fatal blow in the long run. In case of that the infrastructure is damaged, it is hard for emergency response systems to do the job properly (Haskel and Martin, 1993; Kornai, 1980; Qian, 1994).
- Resource constraints – National infrastructure: Governmental systems and social economic systems such as financial systems and public systems are vulnerable to cyber attacks and terror. Those systems provide resources needed to other sub-infrastructures and coordinate allocation of resources. This role encourages terrorists to get their targets on these systems (Haskel and Martin, 1993; Kornai, 1980; Qian, 1994).
- Timing – lags and delays: Early risk detection is essential for being able to address the most important information in a persistent and prospective manner. Early risk detection includes the identification, characterization, evaluation and dissemination of information on possible risks as well as the circumstances of appearance and distribution. The greater the lags and the more rigid the adjustment of supply to changes in the initial demand, the more intensive the shortage will be: the consumer is forced to search more, accept more forced substitution, and so on (Kornai, 1980; Qian, 1994; Wiedemann, Clauberg, Karger, and Henseler, forthcoming).
- Resource constraints – Resource organizing: Under the resource constrained, performance of a system or a society depends on how well resources are organized. In order to organize the constrained resources, it needs sufficient information on resources, sophisticated tools integrating, analyzing, and learning the information, and flexible and coordinated organizations (Kornai, 1980).

In addition, to the above issues, prior literature has articulated the following concerns that are pertinent in the emergency arena.

- Information overload: This is the state of having too much information to make a decision or remained informed about a topic. Lack of a method for comparing and processing different kinds of information can all contribute to this effect (Angus and Daniel, 1974). Under time-constrained situations, information overload often leads to incorrect reactions.
- Privacy concerns: Some studies on economics of privacy have exhibited that when information about customers' tastes and purchase history is available and can be shared among sellers, market laws alone might produce Pareto optimal outcomes (Acquisti, 2004).
- Public fear: This is itself a cost, and it is associated with many other costs, in the form of ripple effects produced by fear. Fear reduction is a critical issue, if the benefits of the response can be shown to outweigh the costs (Sunstein, 2003). Public fear as well as physical damages of infrastructure is a threat to the whole system. Public fear makes it hard to operate various social systems including emergency response systems.

RISK ISSUES

The research question raised here is how to assess risk with respect to existing emergency response systems. To answer this, we have developed a theory based risk framework which is presented as part of Table 2. The framework is described using seven categories of problems: problem of information sharing (R1), problem of resource allocation (R2), problem of insufficient infrastructure (R3), problem of early detection and response (R4), problem of resource organizing (R5), problem of information handling, security and privacy (R6), and problem of protecting social overhead capital (R7). Each problem has its own sub-categories. To justify our framework of risk, two distinct existing incident management systems are analyzed (Atabakhsh, Larson, Petersen, Violette, and Chen, 2004).

Underlying theoretical background		Citation
Problem		
Risk	Description	Citation
Inadequate and imperfect information (Theory of shortage)		Kornai (1980); Qian (1994)
Problem of information sharing (R1)		
Technical barrier for information sharing (R1.1)	The tools necessary to retrieve, filter, integrate, and intelligently present relevant information have not yet been sufficiently refined.	Atabakhsh et al. (2004); Chen et al. (2003)
Communication barrier for information sharing (R1.2)	State and federal agencies have their own information disconnections. They do not open lines of communication	Atabakhsh et al. (2004); Chen et al. (2003); Hanson (2002)
Regulation barriers to share information (R1.3)	Federal, state, and local regulations require that agreements between agencies within their respective jurisdictions receive advanced approval from their governing hierarchy.	Atabakhsh et al. (2004)
Political barriers to share information (R1.4)	State and federal agencies have their own objectives. Sometime, those objectives conflict each other. Shared information can be limited under its own objectives.	Hanson (2002)
Resource constraints – Input (Theory of shortage)		Kornai (1980); Haskel and Martin (1993); Qian (1994)
Problem of resource allocation (R2)		
Limited physical resources (R2.1)	A society of limited resources can not afford to prepare for each and every conceivable disaster.	Arens and Rosenbloom (2003)
Limited human resources (R2.2)	Supplying human resources, who are capable to deal with emergency situation, is extremely constrained. Experts are not evenly distributed and transferring personnel to the emergent places is very limited.	Arens and Rosenbloom (2003)
Resource constraints – Insufficient infrastructure (Theory of shortage)		Kornai (1980); Haskel and Martin (1993); Qian(1994)
Problem of insufficient local infrastructure (R3a)		
Jamming of communications (R3.1)	In an emergent situation, the surge of calls can paralyze the communications network.	Gilbert, Isenberg, Faecher, Papay, Spielvogel, Woodard, and Badolato (2003)
Reduced reliability of communications (R3.2)	The loss of or degradation of radio communications between all parties responding to an attack makes it hard to respond properly.	Gilbert et al. (2003)
Secure communications infrastructure (R3.3)	Protecting computer systems from intrusion and sabotage and enabling recovery from such disruptions would ensure that emergency response teams operate in safety, free from surveillance and malicious interference.	Arens and Rosenbloom (2003)
Loss of communications capacity (R3.4)	Communications facilities which have access to the Internet are vulnerable for the cyber attack.	Gilbert et al. (2003)
Problem of insufficient national infrastructure (R3b)		
Risk to economic structures (R3.5)	Financial institutes which compose of a lot of computers and network systems are vulnerable to the cyber attacks.	Haimes (2002); Haimes and Horowitz (2004); Wulf et al. (2003)
Risk to social infrastructures and government operations (R3.6)	The cyber attack to the government networks make the operations by the government to be paralyzed.	Haimes (2002); Haimes and Horowitz (2004); Wulf et al. (2003)
Risk to cyber-physical infrastructures (R3.7)	Cyber infrastructures are vulnerable to the direct attack by terrorists.	Haimes (2002); Haimes and Horowitz (2004); Wulf et al. (2003)

Timeliness; Lag and Delays (Theory of Shortage)		Kornai (1980); Qian (1994); Wiedemann et al. (forthcoming)
Problem of early detection and response (R4)		
Loss of control of first responders at the scene (R4.1)	In a terrorist attack, first responders would likely be at greater risk because of their limited ability to determine the cause and extent of the situation they find, while also being compelled to provide immediate aid to the injured and the containment of damages.	Gilbert et al. (2003)
Rapidly deployable sensors and effectors (R4.2)	It is essential to deploy the sensors and effectors quickly so their network autonomously among themselves and communicate with controllers outside the crisis zone.	Arens and Rosenbloom (2003)
Resource constraints – Resource organizing (Theory of Shortage)		Kornai (1980)
Problem of resource organizing (R5)		
Lack of encyclopedic digital collections (R5.1)	Lack of information on geography, environments, resources, and potential response personnel and organizations, together with software systems make it hard to answer to pertinent questions.	Arens and Rosenbloom (2003)
Integrated analysis, fusion, and learning (R5.2)	Learning and training technology must be adapted to determine which people need to perform their jobs at which time and ensure that information is tracked and delivered when appropriate.	Arens and Rosenbloom (2003)
Virtual organizations (R5.3)	Uniting geographically dispersed people, software, and hardware systems into flexible, resilient, dynamic, and coordinated teams would be essential parts of the response in emergency situations.	Arens and Rosenbloom (2003)
Information overload; Economics of privacy		Acquisti (2004); Angus and Daniel (1974)
Problem of information handling, security, and privacy (R6)		
Overload problem (R6.1)	The problem that the government agencies can not handle massive amounts of information.	Chen et al. (2003)
Security issue (R6.2)	Data shared between agencies is secure.	Atabakhsh et al. (2004)
Privacy issue (R6.3)	Data shared between agencies that the privacy of individuals is respected.	Atabakhsh et al. (2004)
Legal framework (R6.4)	Protecting individual privacy and civil liberties while resolving the jurisdictional and legal barriers that hamper or even prevent necessary and proper information gathering and sharing by governmental and other organizations during unexpected events.	Arens and Rosenbloom (2003)
Public fear		Sunstein (2003)
Problem of protecting social capital (R7)		
Risk to human lives and psychological unrest in society (R7.1)	Public fear is itself a cost, and it is associated with many other costs, in the form of ripple effects produced by fear.	Haimes (2002); Haimes and Horowitz (2004); Sunstein (2003); Wulf et al. (2003)

Table 2. Risk Framework in Emergency Management Situation

In this study, two example systems are discussed: Urban Search & Rescue (US&R) Task Forces of the National Resource Typing System in the NIMS[3] and biological detection systems.[4]

Further, we apply the risk framework (Table 2) to the two systems. The first case is the Urban search-and-rescue (US&R) Task Force of the National Resource Typing System in NIMS. Urban search-and-rescue (US&R) involves the location, rescue, and initial medical stabilization of victims trapped in confined spaces. Structural collapse is most often the cause of victims being trapped, but victims may also be trapped in transportation accidents, mines and collapsed trenches. Urban search-and-rescue is considered a "multi-hazard" discipline, as it may be needed for a variety of emergencies or disasters,

[3] U.S. Department of Homeland Security (2004).

[4] Fatah, et al. (2001).

including earthquakes, hurricanes, typhoons, storms and tornadoes, floods, dam failures, technological accidents, terrorist activities, and hazardous materials releases (FEMA, 2003).

The second example is that of biological detection systems. It is a detection system against biological terrorism, developed by the Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology (NIST) and working with National Institute of Justice (NIJ) (Fatah et al., 2001). The results are shown in Table 3 & 4.

Component	Metric	Description	Risks	Situation
Personnel	Number of people per response	70 person response	R2.1	Limited manpower can not afford to prepare for every conceivable incident
Personnel	Areas of specialization	Technical level in area of specialty	R4.1	The person who is exposed to an incident is likely to be at great risk because of her/his limited ability to determine the cause and the extent of the situation.
Personnel	Sustained operations	24-hour S&R operations. Self-sufficient for first 72 hours	R6.1	Overload operations might make the person not to make good decisions and respond correctly.
Personnel	Organization	Multi-disciplinary organization	R1.1	Multi-disciplinary organization often suffers from lack of information sharing and different patterns of communication.
Equipment	Sustained operations	Potential mission duration of up to 10 days	R2.1	Low probability and high impact incidents require a lot of equipment at the same time.
Equipment	Communications equipment		R3.4, R3.2	Loss of communication link, congestion of communication channels or overloading on the network hinders relevant operations.
Equipment	Rescue (Medical, Technical, Logistics) equipments		R2.1	It is hard to keep enough equipment to deal with every incident in every place.

Table 3. Example of Risk Assessment of Urban Search & Rescue Task Forces of the National Resource Typing System (Type I)

Source: U.S. Department of Homeland Security (2004).

Components	Description	Risks	Situations
Trigger/Cue	Determine any change in particulate background at the sensor	R4.2	It is essential to deploy the sensors and effectors to detect any changes in a certain area.
Collector	Sampling; for example, sample containing particulates suspended in water	R2.1	Insufficient resources make it hard to respond in case of t incidents occur in many places
Detector	Check if the particulates are biological or inorganic in origin. If they are, they are passed through to the next level of analysis. Otherwise, they are not passed to the next analysis to conserve analytical consumables.	R5.2	The advent of the unexpected biological agents needs various experts in the multi-discipline area.
Identifier	Identify the type of biological agents	R1.1	Incomplete information leads to incorrect decisions. Lack of information sharing might hinder the right judgment.

Table 4. Example of Risk assessment of Components of Biological Detection System Components

Source: Fatah et al. (2001).

CONCLUSIONS

This paper provides an analysis of the existing work. Based on the review of previous literature, in this paper we have proposed a risk framework of the emergency response systems. This framework provides an approach to assess the risks on incident management systems and emergency response systems. Proof of concept is demonstrated by applying the risk framework to two existing incident management systems. The framework shows the components of the incident management systems and the risk items on those incident management systems.

A limitation of the methodology is the lack of a quantitative metric meaning to say the methodology does not show the results through a quantitative measure. The measure of discriminant validity between lists of risk is essential to justify our research results. To effectively mitigate multi-incident coordinated terrorist threats, it is important to consider risk in incident management systems. This paper represents one of the first efforts to study this area.

REFERENCES

1. Acquisti, A. (2004) Privacy and Security of Personal Information: Technological Solutions and Economic Incentives, In *The Economics of Information Security*(Eds, Camp, J. and Lewis, R.) Kluwer.
2. Angus, R. C. and Daniel, T. C. (1974) Applying Theory of Signal Detection in Marketing: Product Development and Evaluation, *American Journal of Agricultural Economics*, 56**,** 3, 573-577.
3. Apostolakis, G. E. (2004) How Useful Is Quantitative Risk Assessment? *Risk Analysis*, 24**,** 3, 515-520.
4. Arens, Y. and Rosenbloom, P. S. (2003) Responding to the Unexpected, *Communications of the ACM*, 46**,** 9, 33-35.
5. Atabakhsh, H., Larson, C., Petersen, T., Violette, C., and Chen, H. (2004) Information Sharing and Collaboration Policies within Government Agencies, *Proceedings of Symposium on Intelligence and Security Informatics*, Tucson, AZ.
6. Atabakhsh, H., Schroeder, J., Chen, H., Chau, M., Xu, J. J., Zhang, J., and Bi, H. (2001) COPLINK Knowledge Management for Law Enforcement: Text Analysis, Visualization and Collaboration, *Proceedings of National Conference on Digital Government*, Los Angeles, CA.
7. Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W., and Schroeder, J. (2003) COPLINK: Managing Law Enforcement Data and Knowledge, *Communications of the ACM*, 46**,** 1, 28-34.
8. Deisler, P. F. (2002) A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism, *Risk Analysis*, 22**,** 3, 405-413.
9. Farrow, S. (2004) Using Risk Assessment, Benefit-Cost Analysis, and Real Options to Implement a Precautionary Principle, *Risk Analysis*, 24**,** 3, 727-735.
10. Fatah, A. A., Barrett, J. A., Arcilesi, R. D., Ewing, K. J., Lattin, C. H., and Helinski, M. S. (2000) Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders, National Institute of Justice.
11. Fatah, A. A., Barrett, J. A., Arcilesi, R. D., Ewing, K. J., Lattin, C. H., and Moshier, T. F. (2001) An Introduction to Biological Agent Detection Equipment for Emergency First Responders, National Institute of Justice.
12. Federal Emergency Management Agency (FEMA) (2003) National urban search and rescue (US&R) response system - Field operations guide, U.S. Department of Homeland Security.
13. Gilbert, P. H., Isenberg, J., Faecher, G. B., Papay, L. T., Spielvogel, L. G., Woodard, J. B., and Badolato, E. V. (2003) Infrastructure issues for cities - Countering terrorist threat, *Journal of Infrastructure Systems*, 9**,** 1, 44-54.
14. Haimes, Y. Y. (1981) Hierarchical holographic modeling, *IEEE Transactions on Systems, Man, Cybernetics*, 11**,** 9, 606-617.
15. Haimes, Y. Y. (2002) Roadmap for modeling risks of terrorism to the homeland, *Journal of Infrastructure Systems*, 8**,** 2, 35-41.
16. Haimes, Y. Y. (2004) Risk modeling, assessment, and management, Wiley, New York.
17. Haimes, Y. Y. and Horowitz, B. M. (2004) Modeling interdependent infrastructures for sustainable counterterrorism, *Journal of Infrastructure Systems*, 10**,** 2, 33-42.
18. Hanson, W. (2002) Bridging the data disconnect: Information sharing essentials, *Government Technology*.
19. Haskel, J. and Martin, C. (1993) Do Skill Shortage Reduce Productivity? Theory and Evidence from the United Kingdom, *The Economic Journal*, 103**,** 417, 386-394.
20. Kornai, J. (1980) Economics of Shortage, North-Holland, Amsterdam.
21. Kunreuther, H. (2002) Risk Analysis and Risk Management in an Uncertain World, *Risk Analysis*, 22**,** 4, 655-664.
22. Paté-Cornell, E. (2002) Fusion of intelligence information: A Bayesian approach, *Risk Analysis*, 22**,** 3, 445-454.
23. Qian, Y. (1994) A Theory of Shortage in Socialist Economics Based on the "Soft Budget Constraint", *The American Economic Review*, 84**,** 1, 145-156.
24. Sunstein, C. R. (2003) Terrorism and probability neglect, *Journal of Risk and Uncertainty*, 26**,** 2/3, 121-136.

25. Turoff, M. (2002) Past and Future Emergency Response Information Systems, *Communications of the ACM*, 45**,** 4, 29-32.
26. U.S. Department of Homeland Security (2004) National Incident Management System,
27. Volonino, L. and Robinson, S. R. (2004) Principles and Practice of Information Security, Prentice-Hall.
28. Wang, G., Chen, H., and Atabakhsh, H. (2004) Automatically detecting deceptive criminal identities, *Communications of the ACM*, 47**,** 3, 71-76.
29. Wiedemann, P. M., Clauberg, M., Karger, C. R., and Henseler, G. (forthcoming) Application of early risk detection concepts and methods of environmental health: A German feasibility study, *Journal of Risk Research.*
30. Wulf, W. A., Haimes, Y. Y., and Longstaff, T. A. (2003) Strategic alternative response to risks of terrorism, *Risk Analysis*, 23**,** 3, 429-444.